REMARKS

Claims 1-4, 6-13, 15-22, and 24-27 are pending in this application. By this Response, claims 1-4, 6-13, 15-22, and 24-27 are amended and claims 5, 14, and 23 are canceled. Claims 1, 10, and 19 are amended to recite defining the e-commerce site as a plurality of security domains and, in response to a user's request to invoke an operation of the e-commerce site, determining a security domain of the plurality of security domains to which the operation relates; selecting a session from a plurality of sessions persisted for the user based on the determined security domain; and reusing the selected session for the user automatically in accordance with the determined security domain. Support for these amendments may be found in canceled claims 5, 14, and 23. Claims 2-4, 6-9, 11-13, 15-18, 20-22, and 24-27 are amended for clarification purposes in view of the amendments to claims 1, 10, and 19. Reconsideration of the claims is respectfully requested in view of the above amendments and the following remarks.

I. Telephone Interview

Applicants thank Examiner Abedin for the courtesies extended to Applicants' representative during the September 12, 2007 telephone interview. During the telephone interview, the above amendments and the distinctions of the claims over the cited art were discussed. With regard to the 35 U.S.C. § 101 rejection of claims 10-13 and 15-18, Examiner Abedin suggested that amending the claims to recite "A computer readable medium..." would overcome the rejection. With regard to the 35 U.S.C. § 102(e) rejection of claims 1-27, Examiner Abedin stated that he would consider Applicants amendments and arguments. The substance of the telephone interview is summarized in the following remarks.

II. 35 U.S.C. § 101, Claims 10-18

The Office Action rejects claims 10-18 under 35 U.S.C. § 101 as being directed towards non-statutory subject matter. By this Response, claim 10 is amended to recite "A computer readable medium tangibly embodying computer executable code for managing multiple user identities for a user of an electronic commerce (e-commerce) site defined using the plurality of security domains, wherein the computer executable code, when executed on a computing device, causes the computing device to:..." Claims 11-13 and 15-18 are amended to recite "The computer readable medium of claim ..." In the Examiner Interview conducted September 12, 2007, the Examiner indicated that amending claims 10-18 in the above manner would overcome the 35 U.S.C. § 101 rejection. Thus, Applicants respectfully request withdrawal of the rejection of claims 10-13 and 15-18 under 35 U.S.C. § 101.

III. 35 U.S.C. § 102, Alleged Anticipation, Claims 1-27

The Office Action rejects claims 1-27 under 35 U.S.C. § 102(e) as being allegedly anticipated by Wood et al. (U.S. Patent No. 6,668,322 B1). This rejection is respectfully traversed.

Amended claim 1, which is representative of the other rejected independent claims 10 and 19 with regard to similarly recited subject matter, reads as follows:

> 1. A method for managing multiple user identities for a user of an electronic commerce (e-commerce) site, the method comprising:
>
> defining the e-commerce site as a plurality of security domains; and
>
> in response to a user's request to invoke an operation of the e-commerce site:
>
> determining a security domain of the plurality of security domains to which the operation relates;
>
> **selecting a session from a plurality of sessions persisted for the user based on the determined security domain; and**
>
> **reusing the selected session for the user automatically in accordance with the determined security domain, the selected being session associated with a user identity and a role, the user identity and the role together indicating privileges for**

invoking operations of the e-commerce site in the determined security domain. (emphasis added)

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). Applicants respectfully submit that Wood does not identically show every element of claim 1 arranged as they are in the claims. Specifically, Wood does not teach the elements emphasized above in claim 1 or similar features in the other rejected independent claims.

Wood is directed to a security architecture that uses a single sign-on. In Wood, session credentials are used to maintain continuity of a persistent session across multiple accesses to one or more information resources, and in some embodiments, across credential level changes. Session credentials are secured, e.g., as a cryptographically secured session token, such that they may be inspected by a wide variety of entities or applications to verify an authenticated trust level, yet may not be prepared or altered except by a trusted authentication service.

Thus, Wood uses session credentials to maintain continuity for one persisted session. Applicants respectfully submit that Wood does not teach **selecting** a session from a plurality of sessions persisted for the user **based on the determined security domain**. The Office Action alleges that Wood teaches selecting one of the sessions in accordance with a determined security domain at column 10, starting at line 30, column 12, starting at line 66 and column 16, starting at line 35, which are reproduced as follows:

> Gatekeeper functionality (e.g., in gatekeeper/entry handler component 110) checks whether a session is already associated with the incoming request. Although other techniques are possible, in some configurations in accordance with the present invention, gatekeeper/entry handler component 110 checks for the presence of a session token in the incoming request. Use of session tokens is described in greater detail below; however, in short, a session token may be, any data supplied to the

client entity for use in uniquely identifying an associated session. In general, preferred session token implementations are cryptographically secured and include facilities, such as expiration or mapping to a particular connection, to limit risk of replay attack and/or spoofing. Some session token implementations may encode session, principal, and/or trust level information. Some session token implementations may employ cookies, URL encoding, or other similar techniques for binding to incoming requests.

(Column 10, lines 30-47)

Browser 170 sends (6) login component 120 a new access request using the URL specified in the redirect from gatekeeper/entry handler component 110. In configurations employing cookies as a medium for passing session tokens, the new access request will include the cookie and therefore the session token. Note that in configurations in which the security architecture controls access to resources in several domains, care should be exercised to select a tag or tags for the cookie such that it will be provided through normal operation of the browser in subsequent accesses to any of the several domains. Persons of ordinary skill in the art will appreciate suitable tagging techniques, including the use of multiple cookies. Login component 120 receives the access request and determines an appropriate authentication scheme based on mapping rules that identify those authentication schemes which are sufficient to achieve a given trust level. Preferably, the mapping rules are a function of environment information. In some configurations, mapping rules are implemented as fuzzy sets wherein acceptable authentication schemes are a function of required trust level and environment information. In this way, environment affects the set of authentication schemes sufficient to meet a trust level requirement.

(Column 12, line 66, to column 13, line 21)

Preferably, gatekeeper/entry handler component 110 supplies an updated session token using a set cookie directive encoded with the results streamed (23A) back to browser 170. An updated session token, if supplied, resolves to the same session object as the session token replaced. As a result, session state (including e.g., identity mappings, authorizations, roles, permissions, environmental variables, etc.) is maintained through the credential level change. However, in the case of a credential upgrade, the session object now encodes a login credential successfully authenticated to achieve a higher trust level. In one advantageous configuration, the achieved (higher) trust level is encoded in a cryptographically secured session token representation as a cookie streamed (23A) back to browser 170 with results (21).

(Column 16, lines 35-49)

In column 10, lines 30-47, Wood describes gatekeeper functionality that checks whether **a session** is already associated with the incoming request using a session token associated with the request. In column 12, line 66, to column 13, line 21, Wood describes that a browser sends a new access request using the URL specified in the redirect from a gatekeeper/entry handler component. The request includes a cookie and therefore a session token. Wood uses the session token to determine an appropriate authentication scheme based on mapping rules that identify those authentication schemes which are sufficient to achieve a given trust level. In column 16, lines 35-49, Wood describes supplying an updated session token and that the updated session token, if supplied, resolves to the **same session** object as the session token replaced.

Thus in these sections, Wood describes a session that is already associated with the session token of the incoming request or a new session is created for the received session token. Applicants respectfully submit that nowhere in these sections, or in any other section of Wood, is there a teaching of maintaining a plurality of sessions that are persisted for the user or **selecting** a session from the plurality of sessions persisted for the user **based on the determined security domain**. That is, in Wood there is only ever one session active at any one time as taught by Wood in column 10, line 48, to column 11, line 11, which is reproduced as follows:

> In some configurations, session tokens are employed **to facilitate session continuity and to allow the security architecture to associate prior authentication of login credentials with an incoming access request**. In one utilization, session tokens are issued to client entities as part of an interaction with the security architecture and are thereafter presented with access requests. In some configurations, **new session tokens (each corresponding to a single session) are issued to client entity on each credential level change**. In other configurations, a session token may remain the same even as credential levels are changed. **Session continuity means the maintenance of coherent session state across one or more interactions between an entity and an information environment**.
>
> Components of session state (e.g., in some configurations, principal id, session id, authenticated trust level, group ids and/or roles, creation time, expiration time, etc.) are maintained or advanced throughout the duration of a session. Typically, aspects of session state are represented internally by the security architecture and a session token (e.g., a session id encoded in a cryptographically secured session token) allows the security architecture to reference into the internal

representation. However, in some configurations, at least some aspects of session state may be represented or duplicated in the session token. For example, a principal id and current trust level are encoded in one realization of a cryptographically secured session credential and associated session token or cookie. **In general, a variety of facilities, such as cookies, can be used to maintain state across a series of protocol interactions, such as HTTP transactions, that do not otherwise support persistent session state.** (emphasis added)

(Column 10, line 48, to column 11, line 11)

In this section, Wood describes that there is only **a single session** persisted or created so that session continuity may be maintained. Wood describes session continuity as the maintenance of coherent session state across one or more interactions between an entity and an information environment. Wood further describes that a variety of facilities can be used to maintain **the session** state across a series of protocol interactions that do not otherwise support persistent session state. Thus, Wood teaches only a single session and Wood does not teach **selecting** a session from a plurality of sessions persisted for the user **based on the determined security domain** as Wood only ever maintains one session for continuity.

Additionally, since Wood does not teach selecting a session from a plurality of sessions persisted for the user based on the determined security domain, Wood does not teach reusing the selected session, which is **selected** from a plurality of sessions persisted for the user **based on the determined security domain**, for the user automatically in accordance with the determined security domain, the selected session being associated with a user identity and a role, the user identity and the role together indicating privileges for invoking operations of the e-commerce site in the determined security domain.

Therefore, Wood does not teach each and every feature of independent claims 1, 10, and 19 as is required under 35 U.S.C. § 102(e). At least by virtue of their dependency on independent claims 1, 10, and 19, the specific features of dependent claims 2-4, 6-9, 11-13, 15-18, 20-22, and 24-27 are not taught by Wood. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-4, 6-13, 15-22, and 24-27 under 35 U.S.C. § 102(e).

Furthermore, Wood does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. Absent the Office Action

pointing out some teaching or incentive to implement Wood such that a session is selected from a plurality of sessions persisted for the user based on the determined security domain and that the selected session, which is selected from a plurality of sessions persisted for the user based on the determined security domain, is reused for the user automatically in accordance with the determined security domain, the selected session being associated with a user identity and a role, the user identity and the role together indicating privileges for invoking operations of the e-commerce site in the determined security domain, one of ordinary skill in the art would not be led to modify Wood to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify Wood in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the Applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

Moreover, in addition to their dependency from independent claims 1, 10, and 19, the specific features recited in dependent claims 2-4, 6-9, 11-13, 15-18, 20-22, and 24-27 are not taught by Wood. For example, with regard to claims 6, 15, and 24, Wood does not teach where the method comprises receiving the user's request in association with the plurality of sessions persisted for the user and retrieving the user identity for the determined security domain from the plurality of sessions. The Office Action alleges that Wood teaches where the method comprises receiving the user's request in association with one or more sessions persisted for the user and retrieving a user identity for the determined security domain from the one or more sessions in column 3, starting at line 1, column 10, starting at line 48, and in claims 1 and 12, which are reproduced as follows:

> In another embodiment in accordance with the present invention, a session token is provided for transfer between a client entity operating on behalf of a principal and a security architecture controlling access to an information resource. The session token includes a principal identifier uniquely identifying the principal and an indication of authorization level accorded by the security architecture after prior authentication of a login credential corresponding to the principal. The principal identifier and authorization level indication are cryptographically secured and allow the security architecture to evaluate sufficiency of the authorization for access

to the information resource without re-authentication of the login credentials.

(Column 3, lines 1-13)

In some configurations, session tokens are employed **to facilitate session continuity and to allow the security architecture to associate prior authentication of login credentials with an incoming access request**. In one utilization, session tokens are issued to client entities as part of an interaction with the security architecture and are thereafter presented with access requests. In some configurations, **new session tokens (each corresponding to a single session) are issued to client entity on each credential level change**. In other configurations, a session token may remain the same even as credential levels are changed. **Session continuity means the maintenance of coherent session state across one or more interactions between an entity and an information environment**.

(Column 10, lines 48-61)

1. A session credential for use in a security architecture controlling access to one or more information resources, the session credential comprising: a principal identifier uniquely identifying a principal; and an encoding of authorization accorded by the security architecture after prior authentication of a login credential corresponding to the principal, the principal identifier and authorization encoding being cryptographically secured and allowing the security architecture to evaluate sufficiency of the authorization for access to the one or more information resources without re-authentication of the login credentials.

(Claim 1)

12. A session token for transfer between a client entity operating on behalf of a principal and a security architecture controlling access to an information resource, the session token comprising: a principal identifier uniquely identifying the principal; and an indication of authorization level accorded by the security architecture after prior authentication of a login credential corresponding to the principal, the principal identifier and authorization level indication being cryptographically secured and allowing the security architecture to evaluate sufficiency of the authorization for access to the information resource without re-authentication of the login credentials.

(Claim 12)

In column 3, lines 1-13, Wood describes a session token that is provided for transfer between a client entity operating on behalf of a principal and a security

architecture controlling access to an information resource. The session token includes a principal identifier uniquely identifying the principal and an indication of authorization level accorded by the security architecture after prior authentication of a login credential corresponding to the principal. In column 10, lines 48-61, Wood describes that there is only a single session that is persisted or created so that session continuity may be maintained. Wood describes that session continuity means the maintenance of coherent session state across one or more interactions between an entity and an information environment. In claim 1, Wood describes a session credential for use in a security architecture controlling access to one or more information resources. In claim 12, Wood describes a session token for transfer between a client entity operating on behalf of a principal and a security architecture controlling access to an information resource. Applicants respectfully submit that none of the sections or claims of Wood teaches receiving a user's request in association with a plurality of sessions persisted for the user and retrieving the user identity for the determined security domain from the plurality of sessions. That is, Wood is merely associated with a single session. Thus, Wood does not need to or provide for retrieving a user identity for a determined security domain from a plurality of sessions.

Thus, in addition to being dependent on independent claims 1, 10, and 19, the specific features of dependent claims 2-4, 6-9, 11-13, 15-18, 20-22, and 24-27 are also distinguishable over Wood by virtue of the specific features recited in these claims. Accordingly, Applicants respectfully request withdrawal of the rejection of dependent claims 2-4, 6-9, 11-13, 15-18, 20-22, and 24-27 under 35 U.S.C. § 102(e).

IV. Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: September 14, 2007

Francis Lammes
Reg. No. 55,353
WALDER INTELLECTUAL PROPERTY LAW, P.C.
P.O. Box 832745
Richardson, TX 75083
(214) 722-6491
AGENT FOR APPLICANTS